arXiv:0909.2598v1 [math.NT] 14 Sep 2009

THE DIVISIBILITY OF $a^n - b^n$ BY POWERS OF n

CHRIS SMYTH

Abstract. For given integers a, b and $j \geq 1$ we determine the set $R_{a,b}^{(j)}$ of integers n for which $a^n - b^n$ is divisible by n^j. For $j = 1, 2$, this set is usually infinite; we determine explicitly the exceptional cases for which a, b the set $R_{a,b}^{(j)}$ $(j = 1, 2)$ is finite. For $j = 2$, we use Zsigmondy's Theorem for this. For $j \geq 3$ and $\gcd(a, b) = 1$, $R_{a,b}^{(j)}$ is probably always finite; this seems difficult to prove, however.

We also show that determination of the set of integers n for which $a^n + b^n$ is divisible by n^j can be reduced to that of $R_{a,b}^{(j)}$.

1. Introduction

Let a, b and j be fixed integers, with $j \geq 1$. The aim of this paper is to find the set $R_{a,b}^{(j)}$ of all positive integers n such that n^j divides $a^n - b^n$. For $j = 1, 2, \ldots$, these sets are clearly nested, with common intersection $\{1\}$. Our first results (Theorems 1 and 2) describe this set in the case that $\gcd(a, b) = 1$. In Section 4 we describe (Theorem 15) the set in the general situation where $\gcd(a, b)$ is unrestricted.

Theorem 1. *Suppose that* $\gcd(a, b) = 1$. *Then the elements of the set* $R_{a,b}^{(1)}$ *consist of those integers* n *whose prime factorization can be written in the form*

$$n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} \quad (p_1 < p_2 < \cdots < p_r, \ \textit{all } k_i \geq 1), \tag{1}$$

where $p_i \mid a^{n_i} - b^{n_i}$ $(i = 1, \ldots, r)$, *with* $n_1 = 1$ *and* $n_i = p_1^{k_1} p_2^{k_2} \ldots p_{i-1}^{k_{i-1}}$ $(i = 2, \ldots, r)$.

In this theorem, the k_i are arbitrary positive integers. The result is essentially contained in [10], which described the indices n for which the generalised Fibonacci numbers u_n are divisible by n. However, we present a self-contained proof in this paper.

On the other hand, for $j \geq 2$, the exponents k_i are more restricted.

Theorem 2. *Suppose that* $\gcd(a, b) = 1$, *and* $j \geq 2$. *Then the elements of the set* $R_{a,b}^{(j)}$ *consist of those integers* n *whose prime factorization can*

2000 *Mathematics Subject Classification.* Primary 11B37, Secondary 11D61.
Key words and phrases. Divisibility, Zsigmondy's Theorem, $a^n - b^n$.

be written in the form (1), where

$$p_1^{(j-1)k_1} \text{ divides } \begin{cases} a-b & \text{if } p_1 > 2; \\ \operatorname{lcm}(a-b, a+b) & \text{if } p_1 = 2, \end{cases}$$

and $p_i^{(j-1)k_i} \mid a^{n_i} - b^{n_i}$, *with* $n_i = p_1^{k_1} p_2^{k_2} \dots p_{i-1}^{k_{i-1}}$ $(i = 2, \dots, r)$.

Thus we see that construction of $n \in R_{a,b}^{(j)}$ depends upon finding a prime p_i not used previously with $a^{n_i} - b^{n_i}$ being divisible by p_i^{j-1}. This presents no problem for $j = 2$, so that $R_{a,b}^{(2)}$, as well as $R_{a,b}^{(1)}$, are usually infinite. See Section 5 for details, including the exceptional cases when they are finite. However, for $j \geq 3$ the condition $p_i^{j-1} \mid a^{n_i} - b^{n_i}$ is only rarely satisfied. This suggests strongly that in this case $R_{a,b}^{(j)}$ is always finite for $\gcd(a, b) = 1$. This seems very difficult to prove, even assuming the ABC Conjecture. A result of Ribenboim and Walsh [9] implies that, under ABC, the powerful part of $a^n - b^n$ cannot often be large. But this is not strong enough for what is needed here. On the other hand, $R_{a,b}^{(j)}$ $(j \geq 3)$ can be made arbitrarily large by choosing a and b such that $a - b$ is a powerful number. For instance, choosing $a = 1 + (q_1 q_2 \dots q_s)^{j-1}$ and $b = 1$, where $q_1, q_2, \dots, q_s$ are distinct primes, then $R_{a,b}^{(j)}$ contains the 2^s numbers $q_1^{\varepsilon_1} q_2^{\varepsilon_2} \dots q_s^{\varepsilon_s}$ where the ε_i are 0 or 1. See Example 7 in Section 7.

In the next section we give preliminary results need for the proof of the theorem. We prove it in Section 3. In Section 4 we describe (Theorem 15) $R_{a,b}^{(j)}$, where $\gcd(a, b)$ is unrestricted. In Section 5 we find all a, b for which $R_{a,b}^{(2)}$ is finite (Theorem 16). In Section 6 we discuss the divisibility of $a^n + b^n$ by powers of n. In Section 7 we give some examples, and make some final remarks in Section 8.

2. Preliminary results

We first prove a version of Fermat's Little Theorem that gives a little bit more information in the case $x \equiv 1 \pmod p$.

Lemma 3. *For $x \in \mathbb{Z}$ and p an odd prime we have*

$$x^{p-1} + x^{p-2} + \dots + x + 1 \equiv \begin{cases} p \pmod{p^2} & \text{if } x \equiv 1 \pmod p; \\ 1 \pmod p & \text{otherwise}. \end{cases} \tag{2}$$

Proof. If $x \equiv 1 \pmod p$, say $x = 1 + kp$, then $x^j \equiv 1 + jkp \pmod{p^2}$, so that

$$x^{p-1} + x^{p-2} + \dots + x + 1 \equiv p + kp \sum_{j=0}^{p-1} j \equiv p \pmod{p^2}. \tag{3}$$

Otherwise

$$x(x-1)(x^{p-2} + \dots + x + 1) = x^p - x \equiv 0 \pmod p, \tag{4}$$

so that for $x \not\equiv 1 \pmod p$ we have $x(x^{p-2} + \cdots + x + 1) \equiv 0 \pmod p$, and hence

$$x^{p-1} + x^{p-2} + \cdots + x + 1 \equiv x(x^{p-2} + \cdots + x + 1) + 1 \equiv 1 \pmod p. \tag{5}$$

□

The following is a result of Birkoff and Vandiver [2, Theorem III]. It is also special case of Lucas [8, p. 210], as corrected for $p = 2$ by Carmichael [3, Theorem X].

Lemma 4. *Let* $\gcd(a, b) = 1$ *and* p *be prime with* $p \mid a - b$. *Define* $t > 0$ *by* $p^t \| a - b$ *for* $p > 2$ *and* $2^t \| \operatorname{lcm}(a - b, a + b)$ *if* $p = 2$. *Then for* $\ell > 0$

$$p^{t+\ell} \| a^{p^\ell} - b^{p^\ell}. \tag{6}$$

On the other hand, if $p \nmid a - b$ *then for* $\ell \geq 0$

$$p \nmid a^{p^\ell} - b^{p^\ell}. \tag{7}$$

Proof. Put $x = a/b$. First suppose that p is odd and $p^t \| a - b$ for some $t > 0$. Then as $\gcd(a, b) = 1$, b is not divisible by p, and we have $x \equiv 1 \pmod{p^t}$. Then from

$$a^p - b^p = (a - b)b^{p-1}(x^{p-1} + x^{p-2} + \cdots + x + 1) \tag{8}$$

we have by Lemma 3 that $p^{t+1} \| a^p - b^p$. Applying this result ℓ times, we obtain (6).

For $p = 2$, we have $p^{t+1} \| a^2 - b^2$ and from $a^2 \equiv b^2 \equiv 1 \pmod 8$, we obtain $2^1 \| a^2 + b^2$, and so $p^{t+2} \| a^4 - b^4$. An easy induction then gives the required result.

Now suppose that $p \nmid a - b$. Since $\gcd(a, b) = 1$, (7) clearly holds if $p \mid a$ or $p \mid b$, as must happen for $p = 2$. So we can assume that p is odd and $p \nmid b$. Then $x \not\equiv 1 \pmod p$ so that, by Lemma 3 and (8), we have $p \nmid a^p - b^p$. Applying this argument ℓ times, we obtain (7). □

For $n \in R_{a,b}^{(j)}$, we now define the set $\mathcal{P}_{a,b}^{(j)}(n)$ to be the set of all prime powers p^k for which $np^k \in R_{a,b}^{(j)}$. Our next result describes this set precisely. (Compare with [10, Theorem 1(a)]).

Proposition 5. *Suppose that* $j \geq 1$, $\gcd(a, b) = 1$, $n \in R_{a,b}^{(j)}$ *and*

$$a^n - b^n = 2^{e_2'} \prod_{p>2} p^{e_p}, \quad n = \prod_p p^{k_p} \tag{9}$$

and define e_2 *by* $2^{e_2} \| \operatorname{lcm}(a^n - b^n, a^n + b^n)$. *Then*

$$\mathcal{P}^{(1)}(n) = \bigcup_{p \mid a^n - b^n} \{p^k, k \in \mathbb{N}\}, \tag{10}$$

and for $j \geq 2$

$$\mathcal{P}_{a,b}^{(j)}(n) = \bigcup_{p : p^{j-1} \mid a^n - b^n} \left\{ p^k : 1 \leq k \leq \lfloor \frac{e_p - jk_p}{j - 1} \rfloor \right\}. \tag{11}$$

Note that e_2 is never 1. Consequently, if $2m \in R_{a,b}^{(2)}$, where m is odd, then $4m \in R_{a,b}^{(2)}$. Also, $2 \in R_{a,b}^{(j)}$ for $j \leq 3$ when $a-b$ is even.

Proof. Taking $n \in R_{a,b}^{(j)}$ we have, from (9) and the definition of e_2 that $jk_p \leq e_p$ for all primes p. Hence, applying Lemma 4 with a, b replaced by a^n, b^n we have for p dividing $a^n - b^n$ that for $\ell > 0$

$$p^{e_p+\ell} \| a^{np^\ell} - b^{np^\ell}. \tag{12}$$

So $(np^\ell)^j \mid a^{np^\ell} - b^{np^\ell}$ is equivalent to $j(k_p + \ell) \leq e_p + \ell$, or $(j-1)\ell \leq e_p - jk_p$. Thus we obtain (10) for $j \geq 2$, with ℓ unrestricted for $j = 1$, giving (10).

On the other hand, if $p \nmid a^n - b^n$, then by Lemma 4 again, $p^\ell \nmid a^{np^\ell} - b^{np^\ell}$, so that certainly $(np^\ell)^j \nmid a^{np^\ell} - b^{np^\ell}$. □

We now recall some facts about the order function ord. For m an integer greater than 1 and x an integer prime to m, we define $\mathrm{ord}_m(x)$, the *order of x modulo m*, to be the least positive integer h such that $x^h \equiv 1 \pmod{m}$. The next three lemmas, containing standard material on the ord function, are included for completeness.

Lemma 6. *For $x \in \mathbb{N}$ and prime to m we have $m \mid x^n - 1$ if and only if $\mathrm{ord}_m(x) \mid n$.*

Proof. Let $\mathrm{ord}_m(x) = h$, and assume that $m \mid x^n - 1$. Then as $m \mid x^h - 1$, also $m \mid x^{\gcd(h,n)} - 1$. By the minimality of h, $\gcd(h, n) = h$, i.e., $h \mid n$. Conversely, if $h \mid n$ then $x^h - 1 \mid x^n - 1$, so that $m \mid x^n - 1$. □

Corollary 7. *Let $j \geq 1$. We have $n^j \mid x^n - 1$ if and only if $\gcd(x, n) = 1$ and $\mathrm{ord}_{n^j}(x) \mid n$.*

Lemma 8. *For $m = \prod_p p^{f_p}$ and $x \in \mathbb{N}$ and prime to m we have*

$$\mathrm{ord}_m(x) = \mathrm{lcm}_p\, \mathrm{ord}_{p^{k_p}}(x). \tag{13}$$

Proof. Put $h_p = \mathrm{ord}_{p^{f_p}}(x)$, $h = \mathrm{ord}_m(x)$ and $h' = \mathrm{lcm}_p\, h_p$. Then by Lemma 6 we have $p^{f_p} \mid x^{h'} - 1$ for all p, and hence $m \mid x^{h'} - 1$. Hence $h \mid h'$. On the other hand, as $p^{f_p} \mid n$ and $m \mid x^h - 1$, we have $p^{f_p} \mid x^h - 1$, and so $h_p \mid h$, by Lemma 6. Hence $h' = \mathrm{lcm}_p\, h_p \mid h$. □

Now put $p_* = \mathrm{ord}_p(x)$, and define $t > 0$ by $p^t \| x^{p_*} - 1$.

Lemma 9. *For $\gcd(x, n) = 1$ and $\ell > 0$ we have $p_* \mid p - 1$ and $\mathrm{ord}_{p^\ell}(x) = p^{\max(\ell - t, 0)} p_*$.*

Proof. Since $p \mid x^{p-1} - 1$, we have $p_* \mid p - 1$, by Lemma 6. Also, from $p^\ell \mid x^{\mathrm{ord}_{p^\ell}(x)} - 1$ we have $p \mid x^{\mathrm{ord}_{p^\ell}(x)} - 1$, and so, by Lemma 6 again, $p_* = \mathrm{ord}_p(x) \mid \mathrm{ord}_{p^\ell}(x)$. Further, if $\ell \leq t$ then from $p^\ell \mid x^{p_*} - 1$ we have by Lemma 6 that $\mathrm{ord}_{p^\ell}(x) \mid p_*$, so $\mathrm{ord}_{p^\ell}(x) = p_*$. Further, by Lemma 4 for $u \geq t$

$$p^u \| x^{p^{u-t} p_*} - 1, \tag{14}$$

so that, taking $u = \ell \geq t$ and using Lemma 6, $\operatorname{ord}_{p^\ell}(x) \mid p^{\ell-t}p_*$. Also, if $t \leq u < \ell$, then, from (14), $x^{p^{t-u}p_*} \not\equiv 1 \pmod{p^\ell}$. Hence $\operatorname{ord}_{p^\ell}(x) = p^{\ell-t}p_*$ for $\ell \geq t$. □

Corollary 10. *Let $j \geq 1$. For $n = \prod_p p^{k_p}$ and $x \in \mathbb{N}$ and prime to n we have $n^j \mid x^n - 1$ if and only if* $\gcd(x,n) = 1$ *and*

$$\operatorname{lcm}_p p^{k'_p}p_* \mid \prod_p p^{k_p}. \tag{15}$$

Here the $k'_p = \max(jk_p - t_p, 0)$ are integers with $t_p > 0$.

Note that p_*, k'_p and t_p in general depend on x and j as well as on p.

What we actually need in our situation is the following variant of Corollary 10.

Corollary 11. *Let $j \geq 1$. For $n = \prod_p p^{k_p}$ and integers a, b with* $\gcd(a,b) = 1$ *we have $n^j \mid a^n - b^n$ if and only if* $\gcd(n,a) = \gcd(n,b) = 1$ *and*

$$\operatorname{lcm}_p p^{k'_p}p_* \mid \prod_p p^{k_p}. \tag{16}$$

Here the $k'_p = \max(jk_p - t_p, 0)$ are integers with $t_p > 0$.

This corollary is easily deduced from the previous one by choosing x with $bx \equiv a \pmod{n^j}$.

By contrast with Proposition 5, our next proposition allows us to *divide* an element $n \in R_{a,b}^{(j)}$ by a prime, and remain within $R_{a,b}^{(j)}$.

Proposition 12. *Let $n \in R_{a,b}^{(j)}$ with $n > 1$, and suppose that $p_{\max}$ is the largest prime factor of n. Then $n/p_{\max} \in R_{a,b}^{(j)}$.*

Proof. Suppose $n \in R_{a,b}^{(j)}$, so that (15) holds, with $x = a/b$, and put $q = p_{\max}$. Then, since for every p all prime factors of p_* are less than p, the only possible term on the left-hand side that divides q^{k_q} on the right-hand side is the term $q^{k'_q}$. Now reducing k_q by 1 will reduce k'_q by at least 1, unless it is already 0, when it does not change. In either case (15) will still hold with n replaced by n/q, and so $n/q \in R_{a,b}^{(j)}$. □

Various versions and special cases of Proposition 12 for $j = 1$ have been known for some time, in the more general setting of Lucas sequences, due to Somer [11, Theorem 5(iv)], Jarden [6, Theorem E], Hoggatt and Bergum [5], Walsh [13], André-Jeannin [1] and others. See also Smyth [10, Theorem 3].

In order to work out for which a, b the set $R_{a,b}^{(j)}$ is finite, we need the following classical result. Recall that $a^n - b^n$ is said to have a *primitive prime divisor* p if the prime p divides $a^n - b^n$ but does not divide $a^k - b^k$ for any k with $1 \leq k < n$.

Theorem 13 (Zsigmondy [11]). *Suppose that a and b are nonzero coprime integers with $a > b$ and $a + b > 0$. Then, except when*

- $n = 2$ *and* $a + b$ *is a power of* 2
  or
- $n = 3$, $a = 2$, $b = -1$
  or
- $n = 6$, $a = 2$, $b = 1$,

$a^n - b^n$ *has a primitive prime divisor.*

(Note that in this statement we have allowed b to be negative, as did Zsigmony. His theorem is nowadays often quoted with the restriction $a > b > 0$ and so has the second exceptional case omitted.)

3. Proof of Theorems 1 and 2

Let $n \in R_{a,b}^{(j)}$ have a factorisation (1), where $p_1 < p_2 < \cdots < p_r$ and all $k_i > 0$. First take $j \geq 1$. Then by Proposition 12 $n/p_r^{k_r} = n_r \in R_{a,b}^{(j)}$, and hence

$$(n/p_r^{k_r})/p_{r-1}^{k_{r-1}} = n_{r-1}, \quad \ldots, \quad p_1^{k_1} = n_2, \quad 1 = n_1$$

are all in $R_{a,b}^{(j)}$. Now separate the two cases $j = 1$ and $j \geq 2$ for Theorems 1 and 2 respectively. Now for $j = 1$ Proposition 5 gives us that $p_i \mid a^{n_i} - b^{n_i}$ $(i = 1, \ldots, r)$, while for $j \geq 2$ we have, again from Proposition 5, that

$$p_1^{(j-1)k_1} \text{ divides } \begin{cases} a - b & \text{if } p_1 > 2; \\ \operatorname{lcm}(a - b, a + b) & \text{if } p_1 = 2, \end{cases}$$

and $p_i^{(j-1)k_i} \mid a^{n_i} - b^{n_i}$ $(i = 2, \ldots, r)$. Here we have used the fact that $\gcd(p_i, n_i) = 1$, so that if $p_i^{k_i} \mid (a^{n_i} - b^{n_i})/n_i^2$ then $p_i^{k_i} \mid a^{n_i} - b^{n_i}$ (i.e., we are applying Proposition 5 with all the exponents k_p equal to 0.)

4. Finding $R_{a,b}^{(j)}$ when $\gcd(a, b) > 1$.

For $a > 1$, define the set $\mathcal{F}_a$ to be the set of all $n \in \mathcal{N}$ whose prime factors all divide a. To find $R_{a,b}^{(j)}$ in general, we first consider the case $b = 0$.

Proposition 14. *We have $R_{a,0}^{(1)} = R_{a,0}^{(2)} = \mathcal{F}_a$, while for $j \geq 3$ the set $R_{a,0}^{(j)} = \mathcal{F}_a \setminus S_a^{(j)}$, where $S_a^{(j)}$ is a finite set.*

Proof. From the condition $n^j \mid a^n$, all prime factors of n divide a, so $R_{a,0}^{(j)} \subset \mathcal{F}_a$, say $R_{a,0}^{(j)} = \mathcal{F}_a \setminus S_a^{(j)}$. We need to prove that $S_a^{(j)}$ is finite. Suppose that $a = p_1^{a_1} \ldots p_r^{a_r}$, with p_1 the smallest prime factor of a. Then $n = p_1^{k_1} \ldots p_r^{k_r}$ for some $k_i \geq 0$. From $n^j \mid a^n$ we have

$$k_i \leq \frac{a_i}{j} p_1^{k_1} \ldots p_r^{k_r} \quad (i = 1, \ldots, r). \tag{17}$$

For these r conditions to be satisfied it is sufficient that

$$\sum_{i=1}^{r} k_i \le \frac{\min_{i=1}^r a_i}{j} p_1^{\sum_{i=1}^r k_i}. \tag{18}$$

Now (18) holds if $j = 1$ or 2, as in this case, from the simple inequality $k \le 2^{k-1}$ valid for all $k \in \mathbb{N}$, we have

$$\sum_{i=1}^{r} k_i \le \frac{1}{2} 2^{\sum_{i=1}^r k_i} \le \frac{\min_{i=1}^r a_i}{j} p_1^{\sum_{i=1}^r k_i}. \tag{19}$$

Hence $S_a^{(j)}$ is empty if $j = 1$ or 2.

Now take $j \ge 3$, and let $K = K_a^{(j)}$ be the smallest integer such that $Kp_1^{-K} \le (\min_{i=1}^r a_i)/j$. Then (18) holds for $\sum_{i=1}^r k_i \ge K$, and $S_a^{(j)}$ is contained in the finite set $S'' = \{n \in \mathbb{N}, n = p_1^{k_1} \dots p_r^{k_r} : \sum_{i=1}^r k_i < K\}$. (To compute $S_a^{(j)}$ precisely, one need just check for which r-tuples $(k_1, \dots, k_r)$ with $\sum_{i=1}^r k_i < K$ any of the r inequalities of (17) is violated. □

One (at first sight) curious consequence of the equality $R_{a,0}^{(1)} = R_{a,0}^{(2)}$ above is that $n \mid a^n$ implies $n^2 \mid a^n$.

Now let $g = \gcd(a, b)$ and $a = a_1 g$, $b = b_1 g$. Write $n = Gn_1$, where all prime factors of G divide g and $\gcd(n_1, g) = 1$. Then we have the following general result.

Theorem 15. *The set $R_{a,b}^{(j)}$ is given by*

$$R_{a,b}^{(j)} = \{n = Gn_1 : G \in \mathcal{F}_g, n_1 \in R_{a_1^G, b_1^G}^{(j)} \text{ and } \gcd(g, n_1) = 1\} \setminus R, \tag{20}$$

where R is a finite set. Specifically, all $n = Gn_1 \in R$ have $1 \le n_1 < j/2$ and

$$G = q_1^{\ell_1} \dots q_m^{\ell_m}, \tag{21}$$

where

$$\sum_{i=1}^{m} \ell_i < K_{g^{n_1}}^{(j)}. \tag{22}$$

Here the q_i are the primes dividing g, and $K_{g^{n_1}}^{(j)}$ is the constant in the proof of Proposition 14 above.

Proof. supposing that $n \in R_{a,b}^{(j)}$ we have

$$n^j \mid a^n - b^n \tag{23}$$

and so $n^j \mid g^n(a_1^n - b_1^n)$. Writing $n = Gn_1$, as above, we have

$$n_1^j \mid (a_1^G)^{n_1} - (b_1^G)^{n_1} \tag{24}$$

and

$$G^j \mid g^{Gn_1} \left((a_1^G)^{n_1} - (b_1^G)^{n_1} \right). \tag{25}$$

Thus (23) holds with n, a, b replaced by n_1, a_1^G, b_1^G. So we have reduced the problem of (23) to a case where $\gcd(a, b) = 1$, which we can solve

for n_1 prime to g, along with the extra condition (25). Now, from the fact that $R^{(2)}_{g,0} = \mathcal{F}_g$ from Proposition 14, we have $G^2 \mid g^G$ and hence $G^j \mid g^{Gn_1}$ for all $G \in \mathcal{F}_g$, provided that $n_1 \geq j/2$. Hence (25) can fail to hold for all $G \in \mathcal{F}_g$ only for $1 \leq n_1 < j/2$.

Now fix n_1 with $1 \leq n_1 < j/2$. Then note that by Proposition 14, $G^j \mid g^{Gn_1}$ and hence (23) holds for all $G \in \mathcal{F}_{g^{n_1}} \setminus S$, where S is a finite set of G's contained in the set of all G's given by (21) and (22). □

Note that (taking $n_1 = 1$ and using (25)) we always have $R^{(j)}_{g,0} \subset R^{(j)}_{a,b}$. See example 7 in Section 7.

5. When are $R^{(1)}_{a,b}$ and $R^{(2)}_{a,b}$ finite?

First consider $R^{(1)}_{a,b}$. From Theorem 1 it is immediate that $R^{(1)}_{a,b}$ contains all powers of any primes dividing $a-b$. Thus $R^{(1)}_{a,b}$ is infinite unless $a - b = \pm 1$, in which case $R^{(1)}_{a,b} = \{1\}$. This was pointed out earlier by André-Jeannin [1, Corollary 4].

Next, take $j = 2$. Let us denote by $\mathcal{P}^{(2)}_{a,b}$ the set of primes that divide some $n \in R^{(2)}_{a,b}$ and, as before, put $g = \gcd(a, b)$.

Theorem 16. *The set $R^{(2)}_{a,b} = \{1\}$ if and only if a and b are consecutive integers, and $R^{(2)}_{a,b} = \{1, 3\}$ if and only if $ab = -2$. Otherwise, $R^{(2)}_{a,b}$ is infinite.*

If $R^{(2)}_{a/g,b/g} = \{1\}$ (respectively, $= \{1, 3\}$) then $\mathcal{P}^{(2)}_{a,b}$ is the set of all prime divisors of g (respectively, $3g$). Otherwise $\mathcal{P}^{(2)}_{a,b}$ is infinite.

The application of Zsigmondy's Theorem that we require is the following.

Proposition 17. *If $R^{(2)}_{a,b}$ contains some integer $n \geq 4$ then both $R^{(2)}_{a,b}$ and $\mathcal{P}^{(2)}_{a,b}$ are infinite sets.*

Proof. First note that if $a = 2$, $b = 1$ (or more generally $a - b = \pm 1$) then by Theorem 2, $R^{(2)} = \{1\}$. Hence, taking $n \in R^{(2)}_{a,b}$ with $n \geq 4$ we have, by Zsigmondy's Theorem, that $a^n - b^n$ has a primitive prime divisor, p say. Now if $p \mid n$ then, by applying Proposition 12 as many times as necessary we find $p \mid n'$, where $n' \in R^{(2)}_{a,b}$ and now p is the maximal prime divisor of n'. Hence, by Proposition 12 again, $n'' = n'/p \in R^{(2)}_{a,b}$ and so, from $n' = pn''$ and Proposition 5 we have that $p \mid a^{n''} - b^{n''}$, contradicting the primitivity of p.

Now using Proposition 5 again, $np \in R^{(2)}_{a,b}$. Repeating the argument with n replaced by np and continuing in this way we obtain an infinite sequence $n, np, npp_1, npp_1p_2, \ldots, npp_1p_2 \ldots p_\ell, \ldots$ of elements of $R^{(2)}_{a,b}$, where $p < p_1 < p_2 < \cdots < p_\ell < \ldots$ are primes. □

Proof of Theorem 16. Assume $\gcd(a, b) = 1$, and, without loss of generality, that $a > 0$ and $a > b$. (We can ensure this by interchanging a and b and/or changing both their signs.) If $a - b$ is even, then a and b are odd, and $a^2 - b^2 \equiv 1 \pmod{2^{t+1}}$, where $t \geq 2$. Hence $4 \in R^{(2)}_{a,b}$, by Proposition 5, and so both $R^{(2)}_{a,b}$ and $\mathcal{P}^{(2)}_{a,b}$ are infinite sets, by Proposition 17.

If $a - b = 1$ then $R^{(2)} = \{1\}$, as we have just seen, above.

If $a - b$ is odd and at least 5, then $a - b$ must either be divisible by 9 or by a prime $p \geq 5$. Hence 9 or p belong to $R^{(2)}_{a,b}$, by Proposition 5, and again both $R^{(2)}_{a,b}$ and $\mathcal{P}^{(2)}_{a,b}$ are infinite sets, by Proposition 17.

If $a - b = 3$ then $3 \in R^{(2)}_{a,b}$, and $a^3 - b^3 = 9(b^2 + 3b + 3)$. If $b = -1$ (and $a = 2$, $ab = -2$) or -2 (and $a = 1$, $ab = -2$) then $a^3 - b^3 = 9$ and so, by Theorem 2, so $R^{(2)} = \{1, 3\}$. Otherwise, using $\gcd(a, b) = 1$ we see that $a^3 - b^3 \geq 5$, and so the argument for $a - b \geq 5$ but with a, b replaced by a^3, b^3 applies. □

6. The powers of n dividing $a^n + b^n$

Define $R^{(j)+}_{a,b}$ to be the set $\{n \in \mathbb{N} : n^j \text{ divides } a^n + b^n\}$. Take $j \geq 1$, and assume that $\gcd(a, b) = 1$. (The general case $\gcd(a, b) \geq 1$ can be handled as in Section 4.) We then have the following result.

Theorem 18. *Suppose that $j \geq 1$, $\gcd(a, b) = 1$, $a > 0$ and $a \geq |b|$. Then*

(a) *$R^{(1)+}_{a,b}$ consists of the odd elements of $R^{(1)}_{a,-b}$, along with the numbers of the form $2n_1$, where n_1 is an odd element of $R^{(1)}_{a^2,-b^2}$;*

(b) *If $j \geq 2$ the set $R^{(j)+}_{a,b}$ consists of odd elements of $R^{(j)}_{a,-b}$ only .*

Furthermore, for $j = 1$ and 2, the set $R^{(j)+}_{a,b}$ is infinite, except in the following cases:

- *If $a + b$ is 1 or a power of 2, $(j, a, b) \neq (1, 1, 1)$, when it is $\{1\}$;*
- *$R^{(1)+}_{1,1} = \{1, 2\}$;*
- *$R^{(2)+}_{2,1} = \{1, 3\}$.*

Proof. If n is even and $j \geq 2$, or if $4 \mid n$ and $j = 1$, then $n^j \mid a^n + b^n$ implies that $4 \mid a^n + b^n$, contradicting the fact that, as a and b are not both even, $a^n + b^n \equiv 1$ or $2 \pmod 8$. So either

- n is odd, in which case $n^j \mid a^n + b^n$ is equivalent to finding the odd elements of the set $R^{(j)}_{a,-b}$;
  or
- $j = 1$ and $n = 2n_1$, where n_1 is odd, and belongs to $R^{(1)}_{a^2,-b^2}$.

Now suppose that $j = 1$ or 2. If $a + b$ is ± 1 or $\pm$ a power of 2, then, by Theorem 2, all $n \in R^{(j)}_{a,-b}$ with $n > 1$ are even, so for $j = 2$ there are no $n > 1$ with $n^j \mid a^n + b^n$ in this case. Otherwise, $a + b$ will have an

odd prime factor, and so at least one odd element > 1. By Theorem 16 and its proof, we see that $R^{(2)}_{a,-b}$ will have infinitely many odd elements unless $a(-b) = -2$, i.e. $a = 2$, $b = 1$ (using $a > 0$ and $a \geq |b|$).

For $j = 1$, there will be infinitely many n with $n \mid a^n + b^n$, except when both $a+b$ and a^2+b^2 are 1 or a power of 2. It is an easy exercise to check that, this can happen only for $a = b = 1$ or $a = 1$, $b = 0$. $\square$

If $g = \gcd(a, b) > 1$, then, since $R^{(j)+}_{a,b}$ contains the set $R^{(j)}_{g,0}$, it will be infinite, by Proposition 14. For $j \geq 3$ and $\gcd(a, b) = 1$, the finiteness of the set $R^{(j)+}_{a,b}$ would follow from the finiteness of $R^{(j)}_{a,b}$, using Theorem 16(b).

7. Examples.

The set $R^{(j)}_{a,b}$ has a natural labelled, directed-graph structure, as follows: take the vertices to be the elements of $R^{(j)}_{a,b}$, and join a vertex n to a vertex np as $n \to_p np$, where $p \in \mathcal{P}^{(j)}_{a,b}$. We reduce this to a spanning tree of this graph by taking only those edges $n \to_p np$ for which p is the largest prime factor of np. For our first example we draw this tree (Figure 1).

1. Consider the set

$$\begin{aligned} R^{(2)}_{3,1} =& 1, 2, 4, 20, 220, 1220, 2420, 5060, 13420, 14740, 23620, 55660, \\ & 145420, 147620, 162140, 237820, 259820, 290620, 308660, \\ & 339020, 447740, 847220, 899140, 1210220, \ldots, \end{aligned}$$

(sequence A127103 in Neil Sloane's Integer Sequences website). Now

$$3^{20} - 1 = 2^4 \cdot 5^2 \cdot 11^2 \cdot 61 \cdot 1181,$$

showing that $\mathcal{P}^{(2)}_{3,1}(20) = \{11, 11^2, 61, 1181\}$. Also

$$\begin{aligned} 3^{220} - 1 =& 2^4 \cdot 5^3 \cdot 11^3 \cdot 23 \cdot 61 \cdot 67 \cdot 661 \cdot 1181 \cdot 1321 \cdot 3851 \cdot 5501 \\ & \cdot 177101 \cdot 570461 \cdot 659671 \cdot 24472341743191 \cdot 560088668384411 \\ & \cdot 927319729649066047885192700193701, \end{aligned}$$

so that the elements of $\mathcal{P}^{(2)}_{3,1}(220)$ less than $10^6/220$, needed for Figure 1, are

$$11, 23, 61, 661, 1181, 1321, 3851.$$

2. Now

$$R^{(2)}_{5,-1} = 1, 2, 3, 4, 6, 12, 21, 42, 52, 84, 156, 186, 372, \ldots,$$

whose odd elements give

$$R^{(2)+}_{5,-1} = 1, 3, 21, 609, 903, 2667, 9429, 26187, \ldots.$$

See Section 6.

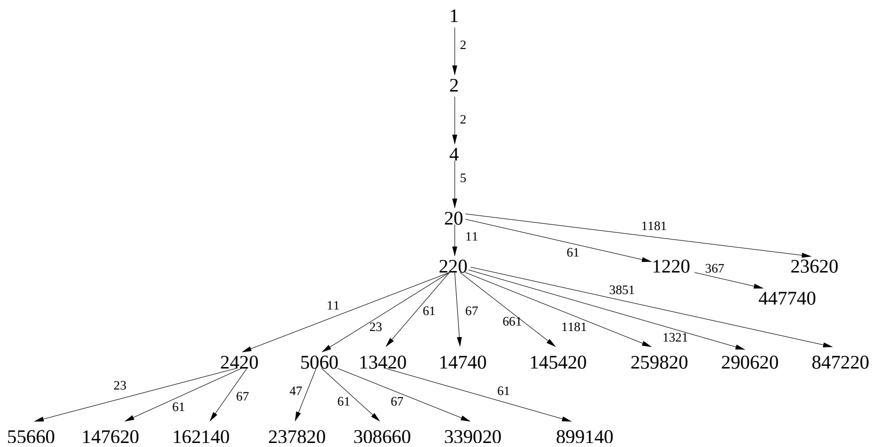

FIGURE 1. Part of the tree for $R^{(2)}_{3,1}$, showing all elements below 10^6.

3. We have
$$R^{(2)+}_{3,2} = R^{(2)}_{3,-2} = 1, 5, 55, 1971145, \ldots,$$
as all elements of $R^{(2)}_{3,-2}$ are odd. Although this set is infinite by Theorem 16, the next term is $1971145p$ where p is the smallest prime factor of $3^{1971145} + 2^{1971145}$ not dividing 1971145. This looks difficult to compute, as it could be very large.
4. We have
$$R^{(2)}_{4,-3} = R^{(2)+}_{4,3} = 1, 7, 2653, \ldots.$$
Again, this set is infinite, but here only the three terms given are readily computable. The next term is $2653p$ where p is the smallest prime factor of $4^{2653} + 3^{2653}$ not dividing 2653.
5. This is an example of a set where more than one odd prime occurs as a squared factor in elements of the set, in this case the primes 3 and 7. Every element greater than 9 is of one of the forms $21m$, $63m$, $147m$, or $441m$, where m is prime to 21.

$$\begin{aligned} R^{(2)}_{11,2} =& 1, 3, 9, 21, 63, 147, 441, 609, 1827, 4137, 4263, 7959, \\ & 8001, 12411, 12789, 23877, 28959, 35931, 55713, 56007, \\ & 86877, 107793, 119973, 167139, 212541, 216237, 230811, \\ & 232029, 251517, 359919, 389403, \ldots, \end{aligned}$$

6. $R^{(4)}_{27001,1} = \{1, 2, 3, 5, 6, 10, 15, 30\}$. This is because $27001 - 1 = 2^3 \cdot 3^3 \cdot 5^3$, and none of $27001^n - 1$ has a factor p^3 for any prime $p > 5$ for any $n = 1, 2, 3, 5, 6, 10, 15, 30$.
7. $R^{(3)}_{19,1} = \{1, 2, 3, 6, 42, 1806\}$? Is this the entire set? Yes, unless $19^{1806} - 1$ is divisible by p^2 for some prime p prime to 1806, in which case $1806p$ would also be in the set. But determining

whether or not this is the case seems to be a hard computational problem.
8. $R^{(4)}_{56,2}$, an example with $\gcd(a,b) > 1$. It seems highly probable that

$$\begin{aligned} R^{(4)}_{56,2} &= (\mathcal{F}_2 \setminus \{2,4,8\}) \cup (3\mathcal{F}_2) \\ &= 1, 3, 6, 12, 16, 24, 32, 48, 64, 96, 128, 192, 256, 384, 512, 768, 1024, \ldots. \end{aligned}$$

However, in order to prove this, Theorem 15 tells us that we need to know that $28^{2^\ell} \not\equiv 1 \pmod{p^3}$ for every prime $p > 3$ and every $\ell > 0$. This seems very difficult! Note that $R^{(4)}_{2,0} = \mathcal{F}_2 \setminus \{2,4,8\}$ and $R^{(4)}_{28,1} = \{1,3\}$.

8. Final remarks.

1. By finding $R^{(j)}_{a,b}$, one is essentially solving the exponential Diophantine equation $x^j y = a^x - b^x$, since any solutions with $x \leq 0$ are readily found.
2. It is known that

$$R^{(1)}_{a,b} = \{n \in \mathbb{N} : n \text{ divides } \frac{a^n - b^n}{a - b}\}.$$

See [10, Proposition 12] (and also André-Jeannin [1, Theorem 2] for some special cases of this result.) This result shows that $R^{(1)}_{a,b} = \{n \in \mathbb{N} : n \text{ divides } u_n\}$, where the u_n are the generalised Fibonacci numbers of the first kind defined by the recurrence $u_0 = 1$, $u_1 = 1$, and $u_{n+2} = (a+b)u_{n+1} - abu_n \, (n \geq 0)$. This provides a link between Theorem 1 of the present paper and the results of [10].

The set $R^{(1)+}_{a,b}$ is a special case of a set $\{n \in \mathbb{N} : n \text{ divides } v_n\}$, also studied in [10]. Here (v_n) is the sequence of generalised Fibonacci numbers of the second kind. For earlier work on this topic see Somer [12].
3. *Earlier and related work.* The study of factors of $a^n - b^n$ dates back at least to Euler, who proved that all primitive prime factors of $a^n - b^n$ were $\equiv 1 \pmod{n}$. See [2, Theorem 1]. Chapter 16 of Dickson [4] (Vol 1) is devoted to the literature on factors of $a^n \pm b^n$.

More specifically, Kennedy and Cooper [7] studied the set $R^{(1)}_{10,1}$. André-Jeannin [1, Corollary 4] claimed (erroneously – see Theorem 18) that the congruence $a^n + b^n \equiv 0 \pmod{n}$ always has infinitely many solutions n for $\gcd(a,b) = 1$.
4. *Acknowledgement.* I thank Hugh Montgomery for telling me about Zsigmondy's Theorem.

References

[1] Richard André-Jeannin. Divisibility of generalized Fibonacci and Lucas numbers by their subscripts. *Fibonacci Quart.*, 29(4):364–366, 1991.

[2] Geo. D. Birkhoff and H. S. Vandiver. On the integral divisors of $a^n - b^n$. *Ann. of Math. (2)*, 5(4):173–180, 1904.

[3] R. D. Carmichael. On the Numerical Factors of Certain Arithmetic Forms. *Amer. Math. Monthly*, 16(10):153–159, 1909.

[4] Leonard Eugene Dickson. *History of the theory of numbers. Vol. I: Divisibility and primality.* Chelsea Publishing Co., New York, 1966.

[5] Verner E. Hoggatt, Jr. and Gerald E. Bergum. Divisibility and congruence relations. *Fibonacci Quart.*, 12:189–195, 1974.

[6] Dov Jarden. Divisibility of Fibonacci and Lucas numbers by their subscripts. In *Recurring sequences: A collection of papers*, Second edition. Revised and enlarged, pages 68–75. Riveon Lematematika, Jerusalem (Israel), 1966.

[7] Robert E. Kennedy and Curtis N. Cooper. Niven repunits and $10^n \equiv 1 \pmod{n}$. *Fibonacci Quart.*, 27(2):139–143, 1989.

[8] Edouard Lucas. Théorie des Fonctions Numériques Simplement Périodiques. *Amer. J. Math.*, 1(3):197–240, 1878.

[9] Paulo Ribenboim and Gary Walsh. The *ABC* conjecture and the powerful part of terms in binary recurring sequences. *J. Number Theory*, 74(1):134–147, 1999.

[10] Chris Smyth. The terms in Lucas sequences divisible by their indices. On arXiv: 0908.3832v1[math.NT], 2009.

[11] Lawrence Somer. Divisibility of terms in Lucas sequences by their subscripts. In *Applications of Fibonacci numbers, Vol. 5 (St. Andrews, 1992)*, pages 515–525. Kluwer Acad. Publ., Dordrecht, 1993.

[12] Lawrence Somer. Divisibility of terms in Lucas sequences of the second kind by their subscripts. In *Applications of Fibonacci numbers, Vol. 6 (Pullman, WA, 1994)*, pages 473–486. Kluwer Acad. Publ., Dordrecht, 1996.

[13] Gary Walsh. On integers n with the property $n \mid f_n$. 5pp., unpublished, 1986.

School of Mathematics and Maxwell Institute for Mathematical Sciences, University of Edinburgh, James Clerk Maxwell Building, King's Buildings, Mayfield Road, Edinburgh EH9 3JZ, UK.